

# Secure rate-adaptive reconciliation

David Elkouss, Jesús Martínez-Mateo and Vicente Martín

Research group on Quantum Information and Computation  
Universidad Politécnica de Madrid (UPM)  
Campus de Montegancedo, 28660 Boadilla del Monte (Madrid), Spain  
e-mail: {delkouss, jmartinez, vicente}@fi.upm.es

**Abstract**—We consider in this paper the problem of information reconciliation in the context of secret key agreement between two legitimate parties, Alice and Bob. Beginning the discussion with the secret key agreement model introduced by Ahlswede and Csiszár, the channel-type model with wiretapper, we study a protocol based on error correcting codes. The protocol can be adapted to changes in the communication channel extending the original source. The efficiency of the reconciliation is only limited by the quality of the code and, while transmitting more information than needed to reconcile Alice's and Bob's sequences, it does not reveal any more information on the original source than an ad-hoc code would have revealed.

## I. INTRODUCTION

Lets start by considering the channel-type model with wire-tapper (CW) for secret key agreement introduced by Ahlswede and Csiszár [1] as shown in Fig. 1. In this model a legitimate party, Bob, and an eavesdropper, Eve, are both connected to another legitimate party, Alice, through a discrete memoryless channel (DMC). Alice generates a discrete sequence of  $n$  values,  $X^n$ , while Bob and Eve observe the correlated outputs,  $Y^n$  and  $Z^n$  respectively, obtained after the transmission of  $X^n$  over the DMC. Both outputs are characterised by transition probability  $P_{Y,Z|X}$ , with each component of the sequences being the outcome of an independent use of the channel. Alice and Bob have also access to a public but authenticated channel used to distill a shared secret key from their correlated sequences. Public and authenticated means in this context that Eve has noiseless access to the information exchanged through the channel, but she is not able to tap the channel without being noticed. Therefore the integrity of the messages on the public channel is guaranteed.

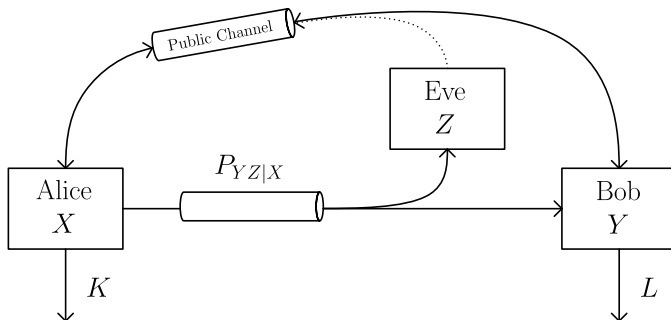


Fig. 1. Ahlswede and Csiszár's model CW.

Protocols that distill a secret key usually divide the distillation process in two different phases. In the first one, known as information reconciliation or simply reconciliation, Alice and Bob exchange redundant information over the public channel in order to eliminate any discrepancy in their correlated sequences,  $X^n$  and  $Y^n$  respectively. At the end of the reconciliation phase both parties have agreed on a shared secret string  $\chi$ , though in many cases  $\chi = X^n$ . On the second phase, known as privacy amplification, Alice and Bob shrink their strings in order to wipe any information of the previously shared key that the eavesdropper could have on  $\chi$  through  $Z^n$  or through any communication over the public channel with information about the strings. This construction allows to split the secret key distillation process into two easier problems. This division is not necessarily suboptimal and, as it is shown in section IV, under certain conditions Alice and Bob can achieve the maximal secret key rate.

The paper is organised as follows: Section II includes a review of the information reconciliation problem linking it with secret key agreement. Section III describes an information reconciliation protocol over an extended string; this protocol uses Wyner's coset scheme with Low-Density Parity-Check (LDPC) codes [2] and can achieve an efficiency as close to its optimum value as allowed by the quality of the code. In section IV it is proved that the proposed protocol does not reveal any more information on  $X$  than an adapted solution for string  $X$  would reveal. And finally, section V analyses the performance of this protocol in a practical scenario.

## II. PROBLEM STATEMENT

Secret key distillation process is usually divided into privacy amplification and information reconciliation. This section defines the meaning of secret key in the context of this paper. Then privacy amplification and information reconciliation are introduced and linked. The objective is to highlight the influence of efficient reconciliation in the achievable secret key rate.

### A. Secret Key Agreement

Alice, Bob and Eve hold  $n$ -length sequences,  $X^n$ ,  $Y^n$  and  $Z^n$  respectively, with each component of the sequences being characterised by  $P_{Y,Z|X}$ .

Let  $\phi_i$  denote the message that Alice sends over the public channel in its  $i$ -th use, and  $\psi_i$  denote the message that Bob

sends in his  $i$ -th use of the channel. Both sets of messages or communications,  $\phi$  and  $\psi$ , are respectively known as forward and backward transmissions. Depending on the protocol any individual message or even  $\phi$  or  $\psi$  might be null. The former case,  $\phi \in \emptyset$ , is known as direct reconciliation while the latter,  $\psi \in \emptyset$ , is known as reverse reconciliation. After  $k$  uses of the public channel, i.e. after the exchange of the set of Alice's first  $k$  messages,  $\phi^k$ , and Bob's,  $\psi^k$  messages, Alice and Bob estimate their shared keys to be  $K$  and  $L$  respectively by using an agreed protocol.

*Definition 1:* A strong secret key rate  $S$  is achievable if there exist  $(\phi^k, \psi^k)$  that for large enough  $n$  and for every  $\epsilon > 0$  that meets simultaneously the following restrictions [3]:

$$\Pr[K \neq L] < \epsilon \quad (1)$$

$$I(\phi^k, \psi^k, Z^n; K) < \epsilon \quad (2)$$

$$H(K) > n \cdot S - \epsilon \quad (3)$$

$$\log |K| < H(K) + \epsilon \quad (4)$$

where  $H(\cdot)$  stands for Shannon's entropy, while  $I(\cdot; \cdot)$  stands for Shannon's mutual information. This definition of secret key rate is strong compared to previous definitions in which the convergence of the conditions was asymptotic and not absolute. In [4] it is shown that both sets of conditions share the same bounds for secret key generation.

Henceforth the superindex indicating length is dropped to reduce the notation, the length of the variable or string should be clear from the context, whenever in doubt we clarify the value that the superindex is taking.

The largest achievable secret rate  $S$  is upper bounded by the secret key capacity,  $C_S$ , which if only forward communications are allowed is defined by [1]:

$$C_{S_f} = \max_{P_{U,X}} [I(U; Y) - I(U; Z)] \quad (5)$$

where  $U$  is an auxiliary random variable that forms the Markov chain  $U \rightarrow X \rightarrow YZ$ .

It should be noticed that  $C_{S_f}$  is a lower bound of  $C_S$  if two way communications are allowed [5]. A case of special interest arises when  $U$  cannot be maximised or  $X$  cannot be manipulated by Alice, an example of this situation is a Quantum Key Distribution (QKD) protocol fixing  $X$  [6]. In this case, taking into account the restrictions, the previous result allows Alice and Bob to achieve at least a secret rate of

$$I(X; Y) - I(X; Z) = H(X|Z) - H(X|Y) \quad (6)$$

where  $H(X|Y)$  and  $H(X|Z)$  are the Shannon conditional entropy.

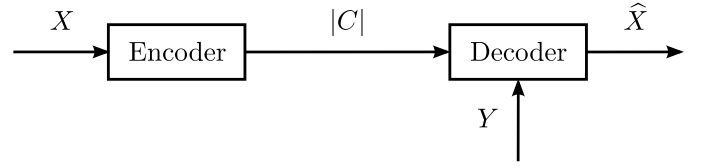


Fig. 2. Source coding with side information.

## B. Privacy Amplification and Information Reconciliation

The problem of privacy amplification —how to reduce  $I(X; Z)$ , the knowledge that Eve might have gathered during the process— has been widely studied. Some of the results on privacy amplification are based on the use of universal families of hash functions [7], however in this work we use extractors [8], proposed by Maurer and Wolf for privacy amplification [4], as they allow to prove the strong secret key rate bounds. An extractor is a function that, with a small amount of random bits acting as catalyst, obtains a number of almost uniformly distributed random bits from a source. The main result, that we develop in section IV, states that given an upper bound on the information the eavesdropper has, Alice and Bob can extract a smaller and highly secret key. The length of the new key is a function of a security parameter and of the upper bound on Eve's information, which in turn depends on: the information that Eve gathers on the private channel and the information that Eve gathers in the information reconciliation phase, directly linking privacy amplification with information reconciliation.

Information reconciliation in the context of secret key agreement is also a well known problem. Once it has been separated from privacy amplification, the problem is reduced to one of Slepian-Wolf coding [9] (see Fig. 2). Given a source  $X$ , it is sufficient a rate  $R \geq H(X)$  to losslessly encode  $X$ , and given two sources  $X$  and  $Y$  to an individual encoding terminal it is sufficient with  $R \geq H(X, Y)$ . The surprising result by Slepian and Wolf states that even for separate encoding  $R \geq H(X, Y)$  is enough [9] and, of particular interest in information reconciliation, that it is also enough for Alice to encode her source  $X$  with  $R \geq H(X|Y)$  in order to allow Bob infer  $X$ .

Wyner's coset scheme is a good solution for the compression of binary sources with side information [10], [11]. The fundamental idea is to assign each source vector to a bin from a set of  $2^{H(X|Y)+\epsilon}$  known bins. The encoder, Alice, transmits the bin number to the decoder, thus encoding  $X$  with rate  $R = H(X|Y) + \epsilon$ . The decoder looks for the source vector inside the described bin with help of the side information  $Y$ .

The efficiency of an information reconciliation protocol sending a sequence  $C$  through the public channel to help Bob recover  $X$  using side information  $Y$  can be measured using a quality parameter  $f$ . If we allow  $|\cdot|$  to stand for the length of a variable,  $f$  is defined by:

$$f = \frac{|C|}{H(X|Y)} \geq 1 \quad (7)$$

According to this definition of efficiency, it takes its lowest value  $f = 1$  in the optimal case, i.e. when the information published for reconciliation is the minimum possible information.

### C. Previous Work

Several protocols have been studied for information reconciliation. Many of them have been discussed in the context of Quantum Key Distribution (QKD) as it is one of the main scenarios of real secret key distillation.

Brassard and Salvail proposed the Cascade protocol in [12] for binary variable reconciliation. Cascade despite being highly interactive remains the most widely used protocol. It offers to its advantage a simple description and a relatively low efficiency value. Other protocols include a protocol by Liu et al. [13] that combines advantage distillation and information reconciliation, and Winnow [14], a protocol in which Alice and Bob exchange the syndrome of a Hamming code for each block.

LDPC codes have been proposed for coding correlated sources in [15], though no explicit codes were given. A rate adaptive construction with non binary LDPC codes was proposed in [16]. On [17] LDPC codes were optimised for the binary symmetric channel (BSC) and used to reconcile binary variables. The efficiency of the codes was close to 1 for crossover probabilities near the codes' thresholds, however as only a discrete number of codes was available the efficiency exhibited a saw behaviour (see Fig. 5). A rate adaptive protocol was proposed in [18], however the security of the protocol was not addressed and the impact of the excess of information on the public channel was not discussed.

## III. RATE ADAPTIVE INFORMATION RECONCILIATION

### A. Formalism

In this section we describe a protocol for the information reconciliation problem based on Wyner's coset scheme, briefly sketched above. Before describing the protocol we review some basic formalism.

Let  $\zeta(n, k)$  be a binary linear code of length  $n$ ,  $k$  information symbols, and  $R_0 = k/n$  its information rate. This code can be specified by a parity matrix  $H$ . Let  $x$  be a  $n$ -length vector, such that  $m(x) = Hx^T$  stands for the syndrome of  $x$ . The code  $\zeta(n, k)$  contains every  $n$ -length vector  $v$  such that  $m(v) = 0$ . The best way to choose the bins for Wyner's schema, is to choose bins with a structure that allows differentiating between them. One natural way is to assign a bin to each coset of a linear code [11]. Each bin can be seen as an affine code, characterised by syndrome  $m_b$ , that contains every  $n$ -length vector  $v$  such that  $m(v) = m_b$ . There are  $2^{n-k}$  different syndromes, thus allowing Alice to encode  $x$  with rate  $(n - k)/n$ .

It was first shown in [19] and generalised in [15] that LDPC codes can be successfully used in order to address the problem of coding correlated sources with side information at the decoder. The message passing decoder must be modified to take into account the different syndromes and, channel coding

techniques that lead to channel capacity approaching codes, lead also to codes approaching the Slepian-Wolf limit [17]. However, a linear code reveals a fixed amount of information independently of the channel characteristics which might not be appropriate in many situations. An scenario with changing statistics can arise in real settings due, for example, to the sensitivity of physical devices or to the presence of an active eavesdropper. To address the problem of secret key agreement when the statistics of the channel can vary from execution to execution, a suitable solution is provided by puncturing and shortening strategies (see Fig. 3).

A punctured code modifies an existing  $\zeta(n, k)$  code by removal of a set of  $p$  from the total  $n$  symbols, thus becoming a code of length  $n - p$  and dimension  $k$ ,  $\zeta'(n - p, k)$ . In the same fashion, a shortened code is a modified code in which  $s$  symbols from the code are known or fixed. A shortened code becomes a code of length  $n - s$  and dimension  $k - s$ ,  $\zeta'(n - s, k - s)$ . A code  $\zeta(n, k)$  in which  $p$  symbols are punctured and  $s$  symbols are shortened becomes a code with rate:

$$R = \frac{k - s}{n - s - p} \quad (8)$$

This expression can also be written as a function of  $R_0$ ,  $\sigma = s/n$  and  $\pi = p/n$ : the original coding rate, the fraction of shortened symbols and the fraction of punctured symbols, respectively. Puncturing and shortening provide the means to adapt the rate of an existing code, however once chosen  $p$  and  $s$  the new rate is fixed. It should also be noted that there is a certain amount of efficiency loss as the percentage of punctured and shortened bits increases and even a limiting threshold of puncturing depending on the code [20].

### B. Rate Adaptive Protocol

The following definition delineates a generic protocol able to adapt the information rate to varying channel parameters through puncturing and shortening strategies,  $s + p$  random bits are added to the original strings. The protocol transmits  $s + n - k$  bits through the public channel, which can stand for the code syndrome and  $s$  shortened bits.

*Definition 2:* Let  $\zeta(n, k)$  be a linear code and  $s, p \in \mathbb{N}$  two parameters such that  $0 \leq s \leq k$ ,  $0 \leq p \leq n$ ,  $s + p \leq n$ . An  $sp$ -protocol allows two parties holding  $x$  and  $y$  two  $(n - p - s)$ -length binary sequences to reconcile their strings. This protocol transmits  $s + n - k$  bits through a public channel and extends both sequences  $x$  and  $y$  with  $s + p$  random bits into  $\hat{x}$  and  $\hat{y}$  two  $n$ -length sequences.

We now describe a practical  $sp$ -protocol which is a formal and simplified version of a protocol described in [18] adapted for easier analysis. Let  $R_0$  be the rate of  $\zeta(n, k)$ , in order to reconcile their string the two parties Alice and Bob perform the following steps:

*Step 0:* Alice and Bob fix a parameter  $\delta = \sigma + \pi$  standing for the number of symbols to either puncture or shorten, this allows them to reconcile the same amount of information on each protocol execution. They characterise as well  $f(p_{\text{err}})$ ,

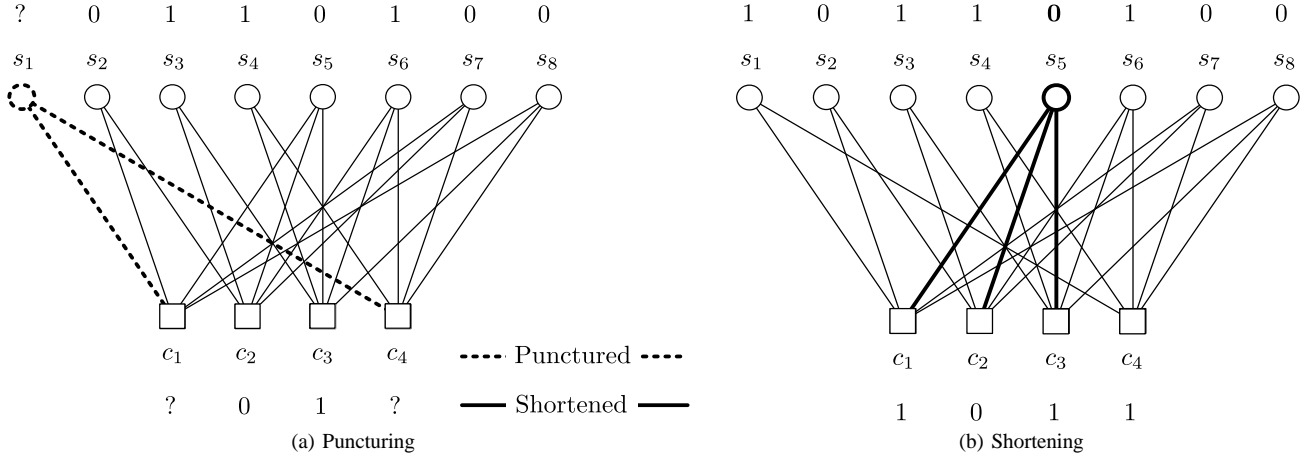


Fig. 3. Example of Tanner graph of an LDPC code with puncturing and shortening strategies applied on only one symbol.

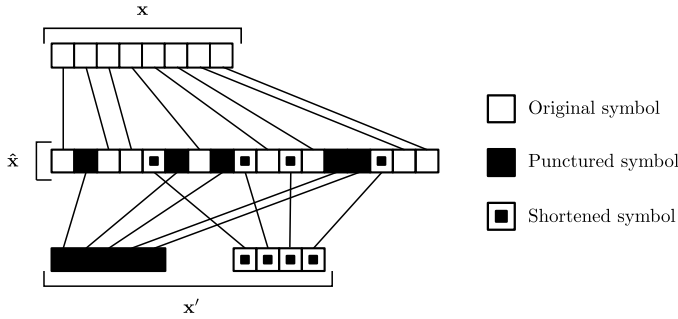


Fig. 4. Extended string construction. It is shown how the extended string  $\hat{x}$  is constructed from a random permutation of two strings: the original string to be reconciled,  $x$ , and a string consisting of punctured symbols,  $x'$ .

the efficiency function describing the behaviour of the code under shortening and puncturing, where  $p_{\text{err}}$  stands for the error probability.

Prior to the execution of the protocol Alice and Bob might have an estimate of the discrepancies between their strings or they might have published and subsequently discarded a subset of their original strings in order to infer the error probability  $p_{\text{err}}$ . Once estimated  $p_{\text{err}}$  and having measured the quality of  $\zeta$  under perforation and shortening, Alice and Bob choose  $s$  and  $p$  such that  $R$  the rate of the equivalent code allows to reconcile both strings with high probability while minimising  $s$ .

*Step 1:* Alice creates an extended string  $\hat{x}$  (see Fig. 4):

$$\hat{x} = g(x|r_A(p)|r_A(s)) \quad (9)$$

where  $g$  is a permutation of  $x|r_A(p)|r_A(s)$ ,  $r_A(p)$  is a random string of length  $p$ , and  $r_A(s)$  is a random string of length  $s$ .

Alice transmits to Bob  $m(\hat{x})$  and  $r_A(s)$ .

*Step 2:* Bob receives Alice message and constructs an extended string  $\hat{y}$ :

$$\hat{y} = g(y|r_B(p)|r_A(s)) \quad (10)$$

where  $r_B(p)$  is a random string of length  $p$  generated by Bob.

Bob recovers  $\hat{x}$  with high probability using the modified belief propagation decoder described in [19].

*Example 1:* Alice and Bob have a code  $\zeta(2 \times 10^5, 10^5)$  with an empirical efficiency below  $f(p_{\text{err}}) \leq 1.09$  in the range  $[0.065, 0.075]$  (see Fig. 5) for  $\delta = 0.05$ . Alice transmits to Bob a string of length  $1.9 \times 10^5$  over a BSC with known crossover probability  $p_{\text{err}} = 0.068$ . In a BSC the conditional entropy can be expressed as  $H(X|Y) = h(p_{\text{err}})$ , and thus the maximum coding rate  $R = 1 - f(p_{\text{err}})h(p_{\text{err}})$ . Then, from Eq. 8, they should puncture  $p = 5,772$  bits and shorten  $s = 4,228$  bits to reconcile their extended strings with high probability and  $f \leq 1.09$ .

An important remark here is that Alice and Bob reconcile their *extended* strings with efficiency  $f$  close to 1, while  $f$ , as defined on Eq. 7 for reconciling the *original* strings, is higher. In the next section we show that the amount of distillable secret bits is not diminished by the higher  $f$  value and, indeed, the relevant figure is the reconciliation efficiency of the extended strings.

#### IV. SECURITY ANALYSIS

The security of  $sp$ -protocols is addressed in this section. As a first step we review the privacy amplification results that allow to take into account the impact of reconciliation in the final key.

We introduce another entropy measure: min-entropy, as it is used in the following discussion. It is defined as:

$$H_\infty(X) = -\log \max_x P_X(x) \quad (11)$$

Generally  $H_\infty(X) \leq H(X)$ , being equal only if  $X$  outcomes are given by a uniform distribution. We further define the conditional min-entropy as:

$$H_\infty(X|Y) = \min_y H_\infty(X|Y=y) \quad (12)$$

*Theorem 1:* Given three constants  $\delta, \Delta_1, \Delta_2 \geq 0$ , after  $n$  uses of a binary symmetric channel ruled by  $P_{Z'|X}$ , if Eve's min-entropy on  $X$  is known to be bounded as  $H_\infty(X|Z' = z') \geq \delta n$ , there exists ([4]) an extractor function  $E : F_2^n \times F_2^u \rightarrow F_2^k$ , with  $u \leq \Delta_1 n$  and  $k \geq (\delta - \Delta_2)n$ , such that if Alice and Bob agree on secret key  $K = E(X, U)$ , where  $U$  is a sequence of  $u$  random uniform bits, the entropy of  $K$  is given by:

$$H(K|U, Z' = z') \geq k - 2^{-n^{1/2 - o(1)}} \quad (13)$$

which wipes all the information from the eavesdropper provided that Alice and Bob can estimate  $H_\infty(K|Z')$ .

The effects of the  $|C|$  redundancy bits shared on the conditional min-entropy can also be bounded using a security parameter  $t$  with probability  $1 - 2^{-t}$  [4]:

$$H_\infty(X|Z' = zc) \geq H_\infty(X|Z = z) - |C| - t \quad (14)$$

measuring the interest of good information reconciliation, every redundancy bit used in this phase reduces the final secret key.

We proceed to demonstrate that the use of an *sp*-protocol does not impose any constraint on the achievable secret key rate. Moreover, from this demonstration it is possible to infer that the quality of the information reconciliation procedure depends only on the quality of the error correction code. We begin with the proof of the following lemma (Lemma 1) that allows to exploit the random construction of the punctured and shortened bits in the proposed protocol.

*Lemma 1:* Let  $X, Y$  and  $Z$  be three random variables, if  $Y$  is independent from variables  $X$  and  $Z$  the mutual min-entropy of  $X$  and  $Y$  conditioned to  $Z$  can be expressed by:

$$H_\infty(XY|Z) = H_\infty(X|Z) + H_\infty(Y) \quad (15)$$

*Proof:*

$$H_\infty(XY|Z) = \min_z H_\infty(XY|Z = z) \quad (16)$$

$$= - \min_z \log \max_{xy} P(xy|z) \quad (17)$$

$$= - \min_z \log \max_{xy} P(x|z)P(y|z) \quad (18)$$

$$= - \min_z \left[ \log \max_x P(x|z) + \log \max_y P(y|z) \right] \quad (19)$$

$$= H_\infty(X|Z) + H_\infty(Y) \quad (20)$$

where Eq. 18 derives from the consideration that  $X$  and  $Y$  being independent variables, and Eq. 20 from  $Y$  and  $Z$  being independent variables. ■

*Theorem 2:* Given a code  $\zeta(n, k)$ , a security constant  $t$ , the public communication  $C$ , and  $Z$  the eavesdropper information,

then the min-entropy of the variable  $\hat{X}$  constructed by the *sp*-protocol, is with probability  $1 - 2^{-t}$  greater or equal than that of using an adapted error correcting code of rate  $R$  to reconcile  $X$  and  $Y$  minus the security constant:

$$H_\infty(\hat{X}|ZC) \geq H_\infty(X|Z) - |X|(1 - R) - t \quad (21)$$

*Proof:*

Directly given by Eq. 14:

$$H_\infty(\hat{X}|ZC) \geq H_\infty(\hat{X}|Z) - |C| - t \quad (22)$$

Distinguishing in  $\hat{X}$  part of the variable that corresponds to the sequence to be reconciled,  $X$ , and the additional variable used to extend the original sequence,  $X'$  (see its correspondence with strings in Fig. 4):

$$= H_\infty(XX'|Z) - |C| - t \quad (23)$$

Since  $X'$  is independent of  $Z$  and  $X$  by construction, Lemma 1 can be applied:

$$= H_\infty(X|Z) + H_\infty(X') - |C| - t \quad (24)$$

The entropy of  $H_\infty(X')$  takes the value of the number of random  $p + s$  bits:

$$= H_\infty(X|Z) + |X| \frac{\pi + \sigma}{1 - \pi - \sigma} - |C| - t \quad (25)$$

The length of the conversation  $|C|$  is  $s + n - k$ , which in the proposed protocol stand for the  $s$  shortened bits and the syndrome of  $X'$ . It can be written as a function of the size of  $X$ ,  $\pi$  and  $\sigma$ :

$$= H_\infty(X|Z) + |X| \frac{\pi + \sigma}{1 - \pi - \sigma} - |X| \frac{(1 - R_0) + \sigma}{1 - \pi - \sigma} - t \quad (26)$$

and thus

$$= H_\infty(X|Z) - |X|(1 - R) - t \quad (27)$$

■

## V. NUMERICAL RESULTS

We discuss the efficiency of several protocols in this section. In order to illustrate the performance of the *sp*-protocol in Fig. 5 we compare the results of adapted LDPC codes to regular LDPC codes without adaptation and to Cascade. We show as well the theoretical efficiency in case of infinite length [18], this curve indicates the expected asymptotic behaviour of the protocol.

Following Theorem 2 two strings can be reconciled with the efficiency of a rate adapted code. In the figure, the efficiency of the punctured and shortened codes is below 1.1 in the whole range of  $p_{\text{err}}$ , close to the theoretical limit. In comparison the codes without adaptation offer a better result close to their threshold but the efficiency quickly drops as the working point moves away from the threshold. On the other hand Cascade exhibits a poorer efficiency on the  $p_{\text{err}}$  range considered.

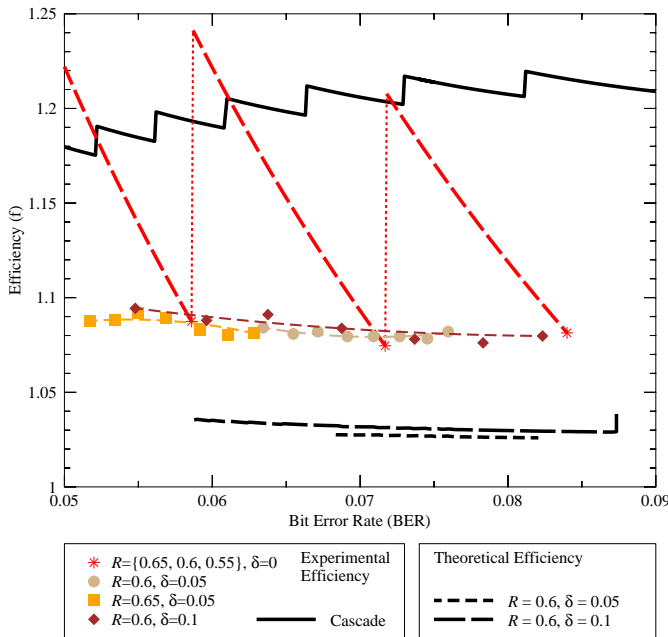


Fig. 5. Reconciliation efficiency of Cascade [12], LDPC codes without puncturing and shortening strategies [17], and the *sp*-protocol in a practical setting as defined in Eq. 7. Two LDPC codes have been chosen to cover the crossover range  $p_{\text{err}} \in [0.055, 0.08]$  using the proposed *sp*-protocol. Both codes,  $\zeta_1(2 \times 10^5, 1.2 \times 10^5)$  with coding rate  $R = 0.6$  and  $\zeta_2(2 \times 10^5, 1.3 \times 10^5)$  with coding rate  $R = 0.65$ , allow to cover the range with  $\delta = 0.05$ , while  $\zeta_2$  with  $\delta = 0.1$  also covers the range of interest. A third code with rate  $R = 0.55$  has been used in order to compare the efficiency of the studied crossover range with a direct strategy, i.e. without using puncturing or shortening, as proposed in [18].

## VI. CONCLUSION

On this paper it has been discussed the problem of information reconciliation in the context of secret key agreement. The *sp*-protocol, a simple protocol based on puncturing and shortening LDPC codes has been proposed. This protocol allows the eavesdropper to gather the same amount of information than an adapted code would reveal; even if it is exchanged more data on the public channel.

It had been argued that information reconciliation based on error correction codes was not optimal for channels with changing characteristics [17], having Alice and Bob access to a discrete set of codes the efficiency of the reconciliation exhibits a saw behavior. The *sp*-protocol allow Alice and Bob to reconcile their chains with a continuous efficiency curve, and as the efficiency of LDPC codes under puncturing and shortening can be analytically described and optimised, the results proved in this paper allow to address the information reconciliation problem as a code design problem. The numerical data on section V indicate that efficiency values close to the theoretical limits can be obtained.

## ACKNOWLEDGMENT

This work has been partially supported by the project Quantum Information Technologies in Madrid<sup>1</sup> (QUITEMAD),

Project P2009/ESP-1594, Comunidad Autónoma de Madrid.

The authors would like to thank the assistance and computation resources provided by Centro de Supercomputación y Visualización de Madrid<sup>2</sup> (CeSViMa).

## REFERENCES

- [1] R. Ahlswede and I. Csiszar, "Common randomness in information theory and cryptography. i. secret sharing," *Information Theory, IEEE Transactions on*, vol. 39, no. 4, pp. 1121–1132, Jul 1993.
- [2] T. Richardson and R. Urbanke, "The capacity of low-density parity check codes under message-passing decoding," *Information Theory, IEEE Transactions on*, vol. 47, pp. 599–618, 2001.
- [3] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Information theoretic security," *Foundations and Trends in Communications and Information Theory*, vol. 5, no. 4–5, pp. 355–580, 2009.
- [4] U. Maurer and S. Wolf, "Information-theoretic key agreement: From weak to strong secrecy for free," in *Lecture Notes in Computer Science*. Springer-Verlag, 2000, pp. 351–368.
- [5] G. Van Assche, "Information-theoretic aspects of quantum key distribution," PhD, Université Libre de Bruxelles, 2005.
- [6] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *International Conference on Computers, Systems and Signal Processing*, Dec. 1984, pp. 175–179.
- [7] C. Bennett, G. Brassard, C. Crépeau, and U. Maurer, "Generalized Privacy Amplification," *Information Theory, IEEE Transactions on*, vol. 41, no. 6, p. 1915, 1995.
- [8] N. Nisan and D. Zuckerman, "Randomness is linear in space," *Journal of Computer and System Sciences*, vol. 52, pp. 43–52, 1993.
- [9] D. Slepian and J. Wolf, "Noiseless coding of correlated information sources," *Information Theory, IEEE Transactions on*, vol. 19, no. 4, pp. 471–480, Jul. 1973.
- [10] A. Wyner, "Recent results in the shannon theory," *Information Theory, IEEE Transactions on*, vol. 20, no. 1, pp. 2–10, 1974.
- [11] R. Zamir, S. Shamai, and U. Erez, "Nested linear/lattice codes for structured multiterminal binning," *Information Theory, IEEE Transactions on*, vol. 48, no. 6, pp. 1250–1276, 2002.
- [12] G. Brassard and L. Salvail, "Secret key reconciliation by public discussion," *Lecture Notes in Computer Science*, vol. 765, pp. 410–423, 1994.
- [13] S. Liu, H. V. Tilborg, and M. V. Dijk, "A practical protocol for advantage distillation and information reconciliation," *Designs, Codes and Cryptography*, vol. 30, no. 1, pp. 39–62, 2003.
- [14] D. Stucki, N. Brunner, N. Gisin, V. Scarani, and H. Zbinden, "Fast and simple one-way quantum key distribution," *Applied Physics Letters*, vol. 87, no. 19, p. 194108, 2005.
- [15] J. Muramatsu, T. Uyematsu, and T. Wadayama, "Low-density parity-check matrices for coding of correlated sources," *Information Theory, IEEE Transactions on*, vol. 51, no. 10, pp. 3645 – 3654, oct. 2005.
- [16] K. Kasai, T. Tsujimoto, R. Matsumoto, and K. Sakaniwa, "Rate-compatible slepian-wolf coding with short non-binary ldpc codes," *Data Compression Conference*, vol. 0, pp. 288–296, 2010.
- [17] D. Elkouss, A. Leverrier, R. Alleaume, and J. J. Boutros, "Efficient reconciliation protocol for discrete-variable quantum key distribution," in *Information Theory, 2009 IEEE International Symposium on*, Jul. 2009, pp. 1879–1883.
- [18] D. Elkouss, J. Martínez, D. Lanco, and V. Martín, "Rate compatible protocol for information reconciliation: An application to qkd," in *IEEE Information Theory Workshop*, Jan. 2010, pp. 145–149.
- [19] A. Liveris, Z. Xiong, and C. Georgiades, "Compression of binary sources with side information at the decoder using ldpc codes," *IEEE Communications Letters*, vol. 6, no. 10, pp. 440–442, 2002.
- [20] H. Pishro-Nik and F. Fekri, "Results on punctured low-density parity-check codes and improved iterative decoding techniques," *Information Theory, IEEE Transactions on*, vol. 53, no. 2, pp. 599–614, Feb. 2007.

<sup>1</sup><http://www.quitemad.org>

<sup>2</sup><http://www.cesvima.upm.es>